IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	)	Criminal No. 1:20-CR-335 (TJM)
	)	
	)	
Petitioner,	)	Speedy Trial Act Exclusion Pursuant to 18 U.S.C. § 3161(h)(1)(D) Through 30 days After Conclusion of Hearing on Pretrial Motions
	)	
v.	)	
	)	**Filed Under Seal**
JACOB DELANEY,	)	
	)	
	)	
Defendant.	)	

GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS

Dated: February 26, 2021

ANTOINETTE T. BACON
Acting United States Attorney

By: /s/ Alicia G. Suarez____
Alicia G. Suarez
Assistant United States Attorney
Bar Roll No. 700218

TABLE OF CONTENTS

INTRODUCTION

On October 29, 2020, a grand jury in the Northern District of New York returned an indictment charging the defendant, Jacob Delaney, with one count of receiving child pornography from in or about September 2018 through on or about December 11, 2019, in violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1), and three counts of possessing child pornography on or about December 12, 2019, in violation of Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2). *See* Dkt. No. 29.

Now before the Court is the defendant's January 29, 2021 motion to suppress all of the physical evidence seized from the subject premises, defendant's residence, on December 12, 2019 pursuant to a federal search warrant issued by Magistrate Judge Daniel J. Stewart on December 10, 2019, including electronic devices containing child pornography, and the Defendant's statements obtained during and after the search, including all recorded and written admissions made by the Defendant. *See* Dkt. Nos. 43, 44, 46-1 and 46-2 at 1.[1]

The defendant claims, (1) that the facts and information provided in the search warrant were insufficient and too stale to establish probable cause to search the defendant's residence and electronic devices for evidence, fruits and instrumentalities of possessing and accessing with the intent to view child pornography, and (2) that the good faith exception to the exclusionary rule does not apply because (a) the application so lacked indicia of probable cause that it was unreasonable to rely upon it, and (b) the applying agent misled the Magistrate Judge by ignoring what the defendant refers to as "established Second Circuit search and seizure law," failing to include critical facts and making unsupported conclusions.

[1] The Defendant's notice of motion was initially filed on January 26, 2021. After addressing sealing and redaction points, the Defendant re-filed the Notice of Motion and supporting documents on January 29, 2021, some of which were filed under seal, on February 1, 2021.

The defendant's arguments fail. First, the accurate facts and information included by the applying agent in the search warrant application and affidavit, made in partial reliance on information provided by a reliable foreign law enforcement agency, provided a substantial basis for the Magistrate Judge to conclude that the Internet user at the subject premises (hereinafter "Target IP Address user") purposely accessed the Target Website, through numerous affirmative steps, with the intention of possessing, or, at a minimum, viewing child pornography. Such facts include that: (1) the Target IP Address user at the subject premises accessed a Tor-based website; (2) that Tor-based website was "dedicated to the sexual exploitation of minor and/or prepubescent males" and regularly included the "advertisement and distribution of child pornography," and (3) because of the nature of Tor, the Internet user accessing the Target Website had to go through numerous steps to seek out that particular child pornography site. Therefore, a fair probability existed that evidence, fruits and instrumentalities of the crimes alleged would be located at the subject premises (also known as the defendant's residence) and on the devices located therein.

Second, even if the application lacked probable cause, which it clearly did not, law enforcement acted in good faith in executing the search warrant and therefore the evidence should not be excluded. The application was not so lacking in probable cause as to make reliance on it unreasonable. Furthermore, the applying agent did not mislead the Magistrate Judge for several reasons. The applying agent's request and Magistrate Judge's findings are consistent with Second Circuit law, as set forth in *United States v. Martin*, *United States v. Falso* and *United States v. Raymonda*, or, at the very least, reasonable minds could differ as to their application. In addition, the defendant fails to show that the applying agent knowingly or recklessly made any material omissions, nor that his findings and conclusory statements, when viewed in light of the totality of the information provided in the application, were misleading. A *Franks* hearing is not warranted

because the defendant failed to make a substantially preliminary showing that the applying agent knowingly, recklessly, or even as a result of gross negligence, made any false or misleading statements.

Finally, the defendant's non-custodial and post-*Miranda* admission that were given during and after the execution of a valid search warrant should not be suppressed.

FACTUAL SUMMARY

On December 10, 2019, United States Magistrate Judge for the Northern District of New York, Daniel J. Stewart, authorized a federal search warrant to search the subject premises, located in New Paltz, New York, the defendant's person, and any computers and electronic storage media located during those searches and to seize evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252A(5)(B) and (b)(2), possessing or accessing with the intent to view child pornography and attempt or conspiracy to do the same. *See* Def. Ex. F (filed under seal). [2] Judge Stewart based his determination on the *totality* of the facts and information provided in an application and affidavit sworn to by FBI Special Agent ("SA"), David Fallon.

SA Fallon's affidavit set forth in detail facts and information—provided by law enforcement agents and analysts, including a reliable foreign law enforcement agency, and known through independent investigation, subpoena responses, surveillance and his training and experience—establishing probable cause that on April 22, 2019, a user of the Internet account at the subject premise accessed a website on the Tor anonymity network dedicated to the sexual exploitation of minor and/or prepubescent males ("Target Website"), and that said Internet account was subscribed to by the defendant at the subject premises. The information sworn to by SA Fallon included, among other information, the following:

[2] All references to "Def. Ex." refer to the exhibits filed by the defendant with his Motion to Suppress, Dkt. No. 44, 46, some of which were redacted and/or filed under seal.

- In August 2019, a foreign law enforcement agency (hereinafter "FLA") "known to the FBI and with a history of providing reliable, accurate information in the past notified, the FBI that FLA determined that on April 22, 2019, a user of IP address 69.206.190.157 accessed online child sexual abuse and exploitation material via a website." *Id.* at ¶ 20.

- SA Fallon further described the FLA as "a national law enforcement agency of a country with an established rule of law" with a long history of sharing "criminal investigative information with U.S. law enforcement," including relating to crimes against children, and that has provided information determined to be reliable relating to IP addresses and the trafficking and possession of child pornography in the U.S. *See id.* at ¶¶ 21-22. The FLA learned information provided in this case through "independent investigation that was lawfully authorized in FLA's country pursuant to its national laws." *Id.* at ¶ 21.

- The Target Website was a Tor-network-based website that launched in approximately 2013 and ceased operating in June 2019. *See id.* at ¶ 15. FLA described the website as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on indecent material of boys." *Id.* at ¶ 20. Elsewhere in the affidavit, the Target Website is described as "dedicated to the sexual exploitation of minor and/or prepubescent males" and notes that "the advertisement and distribution of child pornography and child erotica were regular occurrences on the site." *Id.* at 15. There was a registration page for prospective users to create a username and password, *id.* at ¶, and Target Website users could view "some material without creating an account. However, an account was required to post and access all content," *see id.* at ¶ 20. Account information for the individual using IP address 69.206.190.157 was not included in the affidavit.

- Upon entry to the site, users were presented with various sections. The "video" and "photos" sections offered links to topics such as "adolescents" and "toddlers," with the description of the "toddlers" section including "0-4 years." *See id.* at ¶ 17. Users were also provided with links through forum messages where they could upload and access child pornography and FBI confirmed the existence of images of child pornography. *See id.* at ¶ 18.

- A subpoena response from Charter Communications showed that on November 22, 2019, IP address 69.206.190.157 was registered to the defendant at the subject premises. *See id.* at ¶ 28. Further surveillance and investigation also indicated that the defendant resided at the subject premises. *See id.* at ¶¶ 29-33.

SA Fallon also included information regarding the nature of the anonymous Tor network and how it functions, and the numerous steps an individual has to go through in order to locate a hidden services site such as the Target Website, including installing the appropriate Tor software

and then locating the 16-or-56 character web address for the site, likely through directory sites dedicated to child exploitation related content. *See id.* at ¶¶ 7-14, 22-23. Because the Target Website could only be accessed through the Tor network, SA Fallon explained, based on his training and experience and the nature of Tor, that "it is extremely unlikely that any user could simply stumble upon TARGET WEBISTE without understanding its purpose and content." *Id.* at ¶ 25. Furthermore, based on his prior investigations and training and experience, SA Fallon included characteristics common to such individuals that would go to these lengths to access with the intent to view and/or possess child pornography, which includes possessing and maintaining child pornography images in a digital or electronic form within their residence for many years. *See id.* at ¶¶ 36-37.

On December 12, 2019, law enforcement officers executed the search warrant authorized by Judge Stewart at the defendant's residence in New Paltz, New York. Upon execution of the search warrant, law enforcement seized electronic devices, including a Dell Laptop, KESU hard drive and Cruzer thumb drive from the Defendant's bedroom. *See* Def. Ex. G. An initial forensic preview of the Dell Laptop and KESU hard drive revealed videos and images of minor boys engaged in sexually explicit conduct. *See* Crim. Compl. Aff., Dkt. No. 1, ¶¶ 7-8. Within the KESU hard drive, the videos were in a folder titled "Tor Browser." *Id.*

During the execution of the search warrant, after being told that he was not under arrest and was free to leave, *see* Gov. Ex. 1, ~2:34 (12.19.2019 Delaney Residence Interview, filed under seal), the Defendant admitted that he owned and used the Dell Laptop and provided the password for the laptop, *see id.* at ~9:24. Dkt. No. 1, ¶ 9. The Defendant admitted that he downloaded child pornography from a website and saved the videos of child pornography to his Dell Laptop. *See* Gov. Ex. 1, ~10:19, 13:40. The Defendant voluntarily went with investigators from his residence

to the New York State Police Highland Station. He was again told that he was not in custody and was not handcuffed. *Id.* at ~11:40. Once at the station, the Defendant confirmed that he went with the officers voluntarily to the station and confirmed what he told SA Fallon at his residence. *See* Gov. Ex. 2 (12.19.2019 Delaney Highland Station Interview, filed under seal), ~2:40. SA Fallon read the Defendant his *Miranda* rights during that conversation and the Defendant signed a waiver of rights form and agreed to continue speaking with investigators. *See* Gov. Ex. 2, ~4:45-6:00; Gov. Ex. 3, Waiver of Rights Form, filed under seal. The Defendant described child pornography videos that he viewed and downloaded. *See* Gov. Ex. 2, ~ 7:10-11:00, 13:20-14:30. The Defendant also participated in a post-polygraph, post-*Miranda*, recorded interview in which he made additional admissions regarding his possession of the KESU hard drive and its contents and provided a handwritten statement. *See* Def. Ex. I, filed under seal; Gov. Ex. 4 (12.19.2019 Delaney Pre and Post-Polygraph Interview)

On October 29, 2020, based on evidence presented to the grand jury, a three-count indictment was returned charging the defendant with one count of receiving child pornography and three counts of and possessing child pornography. On January 29, 2021, the defendant filed a motion to suppress the electronic devices seized during the search of his residence on December 12, 2019, including those containing child pornography, as well as the defendant's statements, including his admissions.

ARGUMENT

A. THE PHYSICAL EVIDENCE SEIZED FROM DEFENDANT'S RESIDENCE IS ADMISSIBLE BECAUSE THE SEARCH WAS SUPPORTED BY PROBABLE CAUSE

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the

persons or things to be seized." U.S. Const. amend. IV. Probable cause is "a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Illinois v. Gates*, 462 U.S. 213, 232 (1983).

"The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit[,] . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. Upon review, the affidavit is presumed valid, *United States v. Martin*, 426 F.3d 68, 73 (2d Cir. 2005) (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)). The determination of probable cause by the issuing magistrate is given "great deference," and the reviewing court need only find that the magistrate had a "substantial basis" for concluding that probable cause existed. *Gates*, 462 U.S. at 236, 238-39; *see also United States v. Travisano*, 724 F.2d 341, 345 (2d Cir. 1983). Furthermore, reviewing courts "resolve any doubt about the existence of probable cause in favor of upholding the warrant," *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998).

Courts "may conclude that a warrant lacks probable cause where the evidence supporting it is not sufficiently close in time to the issuance of the warrant that probable cause can be said to exist as of the time of the search—that is, where the facts supporting criminal activity have grown stale by the time that the warrant issues". *United States v. Raymonda*, 780 F.3d 105, 114 (2d 2015 (quotations omitted). However, the Second Circuit has "recognized that the determination of staleness in investigations involving child pornography is unique." *Id.* (citing *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006)). This is "[b]ecause it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes." *Id.* (quotations omitted). Reaching that inference turns on whether "the suspect is a person

interested in images of child pornography," such that he would be prone to the proclivities of a collector of child pornography. *Id.* (quotations and citations omitted).

1. Accessing The Tor-Based Target Website Dedicated To The Advertising And Distribution Of Child Pornography Is Sufficient To Establish Probable Cause

Based on the totality of the circumstances set forth in SA Fallon's December 10, 2019 application and affidavit, the Magistrate Judge had a substantial basis to conclude that evidence, fruits and instrumentalities that the Target IP Address user possessed, or at least accessed with the intent to view, child pornography would be located at the subject premises—defendant's residence—and on electronic devices located therein.

Multiple jurisdictions, including the Second Circuit, have held that evidence of a user's membership to an online child pornography website is sufficient to establish probable cause to obtain a search warrant of the premises of the alleged user when the primary purpose of the website is for the collection and distribution of child pornography because "[i]t is common sense that an individual who joins such a site would more than likely download and possess such material." *See e.g.*, *Martin*, 426 F.3d at 74-75 (finding probable cause where the purpose of the e-group "girls12-16" was to distribute child pornography); *United States v. Shield*, 458 F.3d 269 (3d Cir. 2006) (finding probable cause where defendant voluntarily registered with two e-groups devoted to distributing and collecting child pornography); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004) ("[T]he magistrate was entitled to conclude that the overriding reason someone would join [a child pornography] group was to permit him to receive and trade child pornography.").

Even without membership to such a website, probable cause may be established where "similar circumstances" exist showing that an individual went to a website for the "purpose of finding child pornography." *See Raymonda*, 780 F.3d at 116. In *United States v. Falso*, the Second

Circuit considered whether allegations that the defendant "*appeared*" to "have gained *or* attempted to gain" access to a publicly available website containing approximately eleven images of child pornography, with no evidence that the defendant subscribed to a hidden portion of the website, was sufficient to establish probable cause to search the defendant's residence for evidence of child-pornography related crimes. *See* 544 F.3d 110, 117-121 (2d Cir. 2008). In doing so, the Second Circuit examined its precedential holding and analysis in *Martin*, including its reliance on the defendant's membership to the site at issue in that case and the conclusions drawn based on that membership. *Id.* However, the Second Circuit did not stop its analysis in *Falso* at membership, noting that "nothing in [*Martin*] should be read to require these conditions in all similar cases." *Id.* at 120. Yet, in *Falso*, the Court also distinguished *Martin* observing that unlike in *Martin* there was no allegation that the defendant in *Falso* actually accessed the website at issue, nor did the agent describe the website, establishing that its central purpose was to trade child pornography. *Id.* at 121 (citing *Martin*, 426 F.3d at 75). The Court ultimately found that it was not the lack of membership alone, but the inconclusive statements regarding access, "coupled with the absence of details about the features and nature of the non-member site, [that fell] short of establishing probable cause." *Id.* Later, in *Raymonda*, the Second Circuit made clear that the crux of the analysis for establishing probable cause in these types of cases is not necessarily membership, but whether "similar circumstances" exist showing that the defendant had a "demonstrable interest in" accessing or possessing child pornography. 780 F.3d at 116.

In the present case, while neither SA Fallon, nor the FLA provided registration or "user" information to the Target Website for the Target IP Address user, similar circumstances to membership existed showing that the Target IP Address user had a "demonstrable interest," in

accessing with the intent to view and possessing child pornography, and that the user purposely accessed the Target Website to at least view, if not also possess, child pornography.

First, SA Fallon's affidavit specifically alleged that an Internet user at the defendant's residence *accessed*—not appeared or attempted to gain access to—the Target Website, and therefore child pornography, on April 22, 2019. SA Fallon accurately averred that, in August 2019, the FLA "determined on April 22, 2019, a user of IP address 69.206.190.157 ["Target IP Address"] accessed online child sexual abuse and exploitation material via a website," and went on to identify that website as Target Website. Def. Ex. E at ¶ 20. This not only indicates that the Target IP Address user accessed the Target Website, but also accessed child pornography. This statement is consistent with the contents of a letter sent from the FLA to the FBI. *See* Def. Ex. B (filed under seal). The particular IP address identified by the FLA as accessing the Target Website was later identified as being subscribed to by the defendant at the subject premises, supporting the conclusion that the Target IP Address user at the subject premises accessed the Target Website. *See* Def. Ex. E at ¶¶ 27-28; Def. Ex. C.

The defendant claims that SA Fallon could not make such a representation, or the Magistrate Judge could not reach such a conclusion, because of SA Fallon's description of the Tor network, which was also included at length in the affidavit, *see* Def. Mem., Dkt. No. 44 at 5-7. However, his argument is not supported by the totality of the circumstances set forth in the affidavit. While SA Fallon accurately described the lengths Tor goes to in order to keep users anonymous—including routing communications through multiple nodes resulting in only the exit node, as opposed to the Tor user's actual IP address, appearing on a website's IP address log—, and noted that because of these efforts "traditional IP address-based identification techniques are not effective," that does not mean that there are *no* investigative techniques that would allow law

enforcement to identify a Tor user's IP address, rather than a Tor exit node. In fact, the affidavit supports the opposite conclusion. As is indicated in the affidavit, the FLA, which was known to the FBI and had a history of providing reliable, accurate information, Def. Ex. E at ¶ 19, obtained the Target IP Address during its "independent investigation that was lawfully authorized in [its] country pursuant to its national laws," *id.* at ¶ 21. When taken in its totality, a common-sense reading of the affidavit reasonably leads to the conclusion that the FLA applied some, lawful investigative technique that allowed it to identify the Tor user accessing Target Website—IP address 69.206.190.157—which was the IP address of the actual Tor user and not the IP address of the exit node.[3] *See id.* at ¶¶ 19-22. SA Fallon's description of the Tor network and "traditional" investigative techniques does not nullify this conclusion.

Furthermore, SA Fallon appropriately relied on the statements of the FLA and the findings of its lawful investigation to show that the Internet user at the subject premises accessed the Target Website. As the Eastern District of Virginia recently found when addressing the same underlying FLA investigation,[4] "there is more than a substantial basis for crediting the hearsay [statements of the FLA]," without requiring more. *U.S. v. Sanders*, 1:20-cr-00143 (TSE), Dkt. No. 122, (Oct. 29, 2020, EDVa); *see also Gates*, 462 U.S. at 241-42 ("an affidavit relying on hearsay 'is not deemed insufficient on that' score, so long as a substantial basis for crediting the hearsay is present.'"). "[A] tip from one federal law enforcement agency to another implies a degree of expertise and a

[3] While the Magistrate Judge was not privy to the underlying communications between the FLA and FBI due to the sensitive nature of the FLA's investigation, a letter sent from the [redacted] (the FLA) to the FBI on September 16, 2019 indicates that the NCA provided data to the FBI in relation to IP addresses that were lawfully obtained via two warrants "lawfully authorized under [redacted] laws and that the [redacted] did not access, search or seize any data from any computer in the United States." *See* Def. Ex. B (filed under seal).

[4] It appears based on the court's unsealed, yet redacted order, that the same underlying FLA investigation was at issue in *Sanders*, but that the case at issue there involved a similar, but separate Tor-based website.

shared purpose in stopping illegal activity, because the agency's identity is known." *U.S. v. Benoit*, 730 F.3d 280, 285 (3d Cir. 2013).

Second, like the agent in *Martin*, and unlike the agent in *Falso*, SA Fallon described in detail the objectives and contents of the Target Website as provided by the FLA and other FBI agents, providing a substantial basis to conclude that the site's primary focus was on the advertisement and distribution of child pornography. *See* Martin, 426 F.3d at 74-76 (describing the website's welcome message and contents supported conclusion that the "primary reason for [its] existence, was the trading and collection of child pornography"); *Falso*, 544 F.3d at 121 (noting that the agent's affidavit fell short of providing such a description). For example, SA Fallon explained that "[u]pon entry to the site, users were presented with sections and the "videos and "photos" sections offered links to topics such as "hardcore," "adolescents," and "toddlers," which was described as "0-4 years." Def. Ex. E, ¶ 17. SA Fallon also accurately represented that the FLA indicated that the user of the IP address identified "accessed child sexual abuse and exploitation material via a website," and went onto describe the Target Website as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on indecent material of boys," and that users were able to view some material without creating an account. *Id.* at ¶ 20; *see also* Def. Ex. B at pp. 2-3.[5] SA Fallon also stated, that "[t]he advertisement and distribution of child pornography and child erotica were regular occurrences on this site," *id.* at ¶ 15, and he included an example of such an image, *see id.* at ¶ 18. The information that SA Fallon

[5] The defendant takes issue with the FLA and SA Fallon's use of the term "child abuse material," claiming that it is undefined and not particularized. However, again, when the affidavit is read in total, it is clear that the FLA was including "child sexual abuse" and "child sexual exploitation" (sexually explicit conduct being a defined term in the affidavit) material within that term, and was specifically referencing "images , links and videos" not just text regarding the Target Site. *Compare* Def. Mem., Dkt No. 44, 8-9 and Def. Ex. E., ¶ 20.

provided in the affidavit was consistent with information provided by the FLA, *see* Def. Ex. B,[6] and the lead he received from FBI, *see* Def. Ex. D (filed under seal).

Third, because of the nature of Tor and the fact that the Target Website could only be accessed through Tor, the Magistrate Judge had a substantial basis to conclude that the Target IP Address user *purposely* accessed the Target Website and did so to view and possess child pornography, regardless of whether that individual was a registered user of the Target Website. SA Fallon explained that accessing the Target Website "required numerous affirmative steps," Def. E. E at ¶ 25, including "installing the appropriate Tor software" on the Tor user's computer and finding the "16-or-56 character web address" of the Target Website, *id.* at ¶ 23. He further explained that locating the web address of a hidden service website on Tor is "much more difficult" than performing searches for open Internet websites. *See id.* For this reason, Tor users keep, maintain and use directory sites that advertise the content they are interested in, such as "child exploitation material." *Id.* Those sites then contain clickable hyperlinks to access hidden services containing the content sought, here child pornography. *Id.* As SA Fallon indicated, "the web address for the [Target Website] was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children." *Id.* As such, SA Fallon reasonably concluded, based on the totality of this information and his training and experience that "it is extremely unlikely that any user could simply stumble upon TARGET WEBISTE without understanding its purpose and content." *Id.* at ¶ 25.

Based on the nature of Tor and the Target Website, the arrival of the Target IP Address user at the Target Website "was no mere happenstance." *Sanders*, 1:20-cr-00143 (TSE), Dkt. No.

[6] The government notes that the date reflected on page 2 of [redacted] included in Def. Ex. B was automatically populated the last time the document was opened before provided it to the defendant. That does not reflect the date on which it was provided to the FBI.

122 at 9. Rather, as the court in the Easter District of Virginia found, the numerous affirmative steps required to navigate to the Target Website "warrants the inference that the Target IP Address user's arrival at the Target Website was purposeful, that is the Target IP Address user's purpose was to access the website and its illegal content." *Id.* at 9-10.[7] Therefore, the Magistrate Judge had a substantial basis to conclude that that there was a fair probability that evidence of the crimes alleged would be located at the subject premises and on the electronic devices located therein. To the extent that the defendant suggests that the court should require evidence that the Target IP Address user saved illicit images, that "conflates the standard for issuance of a search warrant—namely fair probability that contraband will be found at the location of the Target IP address—with the standard for conviction of a crime—namely proof beyond a reasonable doubt," and therefore is not appropriate or necessary here. *Id.* at 9; *see also Raymonda*, 780 F.3d at 116 (focusing on the defendant's purpose for visiting the site in drawing reasonable conclusions, as opposed to requiring actual downloads or possession).

Finally, the facts and information establishing probable cause here do not suffer from staleness. As already set forth in detail above, the facts in the affidavit substantially support the conclusion that the Target IP Address user "willfully and deliberately"—not negligently or inadvertently—accessed the Target Website knowing of its purpose and contents, thereby establishing that this "person [was] interested in images of child pornography*." See* 780 F.3d at 114-15. Where, as here, the Target IP Address user's access to child pornography "depended on a series of sufficiently complicated steps to suggest his willful intention to view the files," even if only on one occasion, *id.* at 115 (citing *United States v. Vosburgh*, 602 F.3d 512, 528 (3d Cir. 2010), there was a substantial basis for the Magistrate Judge to conclude that the user's access was

[7] The references to the Target IP Address user in *Sanders* are to the user at issue in that case, but the conclusions equally apply to the case at hand.

"sufficiently deliberate or willful to suggest that he was an intentional 'collector' of child pornography, likely to hoard images," for a lengthy period of time, *id.* at 117. Furthermore, because of the nature of Tor, it is likely that the Target IP address user would have stored information related to the online directories and Target Website on his electronic devices to access them more easily in the future. And, although the FLA only provided one instance in which the Target IP Address user accessed the Target Website, the FBI found in the Tor-based Playpen investigation, involving a child pornography hidden services site, that it was exceedingly rare for a user to access such a site and never return, s*ee* Def. Ex. E, ¶ 24, also supporting the conclusion that the Target IP Address user likely visited sites such as this on more than one occasion, evidence of which would be located on his electronic devices.

These factors substantially support the Magistrate Judge's conclusion that there was a "fair probability" that evidence, fruits and instrumentalities of possession, and at a minimum, accessing the Target Website with the intent to view child pornography, would be found at the subject premises and on the electronic devices located therein.

B. EVEN IF THE SEARCH WARRANT WAS NOT SUPPORTED BY PROBABLE CAUSE, LAW ENFORCEMENT ACTED IN GOOD FAITH AND THE EVIDENCE SHOULD NOT BE SUPPRESSED

As set forth above, the accurate facts and information set forth in SA Fallon's affidavit provided the Magistrate Judge with ample bases to find that a "fair probability" to conduct the search. Even if that were not the case, though, exclusion is not appropriate or warranted here.

Evidence seized pursuant to a search warrant will be admissible even if the warrant lacks probable cause or is subsequently found defective if the executing officers relied upon it in "objective good faith." *United States v. Leon*, 468 U.S. 897, 920–24 (1984). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully

deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009). Further, "suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Leon*, 468 U.S. at 918. "When an officer genuinely believes that he has obtained a valid warrant from a magistrate and executes that warrant in good faith, there is no conscious violation of the Fourth Amendment, 'and thus nothing to deter.'" *Raymonda*, 780 F.3d at 118 (quoting *Leon*, 468 U.S. at 920-21).

The good faith exception does not apply:

> (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

Id. (quotations and citation omitted). None of which exist here.

1. The Affidavit Was Not "So Lacking In Indicia of Probable Cause"

SA Fallon's application and affidavit set forth accurate and detailed facts and information as to the FLA's investigation, the Target IP Address, Target Website, Tor, the subject premises and individuals who possess child pornography, all of which he believed set forth probable cause for the warrant requested. Even if those facts did not establish probable cause, the application was not so lacking in indicia of probable cause to render law enforcement's reliance upon it unreasonable. As is detailed above, SA Fallon's request and application is consistent with, not contradictory to Second Circuit precedent set forth in *Martin*—which the defendant fails to reference—*Falso* and *Raymonda*. Even if this Court determined that were not the case, probable cause involves a fact intensive inquiry where reasonable minds may differ and there are distinguishable facts in the instant case from those in *Falso* and *Raymond*—access, Tor and the

purpose of the Target Website—that at least arguably do not require the same probable cause and staleness finding as in *Falso* and/or *Raymonda*. *See Falso*, 554 F.3d at 128 (acknowledging "the different approaches to the probable cause issue" in that case, as well as the split opinion in *Martin*).[8]

The defendant more generally claims that the application was grossly deficient for other, related reasons (i.e., staleness and lack of affirmative conduct by the Target IP Address user) all of which are similarly unsubstantiated. As is detailed above, contrary to the defendant's claims, the affidavit accurately set forth information showing that the Target IP Address user, at the subject premises, accessed the Target Website—as was stated by the FLA and supported by its lawful investigation—and engaged in conduct on Tor that at least arguably demonstrated a predisposition for collecting child pornography. SA Fallon provided specific, reliable facts from the FLA's investigation, which identified the Target IP Address, as well as the nature of Tor and the Target Website to support the Magistrate Judge's conclusions.

2. The Magistrate Judge Was Not Knowingly Or Recklessly Misled

The Magistrate Judge was not knowingly or recklessly misled, nor misled based on gross negligence, by SA Fallon. "Generally, the way a defendant demonstrates that statements in an affidavit intentionally or recklessly misled a district court is through a *Franks* hearing." *Falso*, 544 F.3d at 125. However, a defendant is only entitled to such a hearing "where he or she makes a 'substantial preliminary showing' that a deliberate falsehood or statement made with reckless disregard for the truth was included in the warrant affidavit and the statement was necessary to the judge's finding of probable cause." *Id.* (quoting *Franks v. Delaware*, 438 U.S. 154, 155-56, 170-

[8] While not necessary to the Court's finding, the Magistrate Judge considered *Martin* and *Falso* prior to issuing the search warrant in this case.

71 (1978). A showing that information on which the determination of probable cause hinged was intentionally omitted from a warrant application also qualifies. *See, e.g.*, *United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003). The defendant has made no such showing here. A hearing is not warranted and exclusion would serve no deterrent purpose.

The defendant makes several broad, unsupported claims that SA Fallon recklessly mislead the Magistrate Judge. The defendant claims that SA Fallon made baseless, conclusory representations that there was probable cause to support the search warrant. However, he does not point to specific conclusory probable cause statements or why those statements were recklessly false or misleading, particularly in light of the extensive facts set forth in the affidavit that supported those conclusions. *See* Def. Mot. at 12; *Franks*, 438 U.S. at 171 ("[t]he challenger's attack must be more than conclusory").

The defendant's attempt at more specific claims also fail. The defendant focuses on what he claims to be two omissions. However, he does not show that SA Fallon knowingly or recklessly omitted either to mislead and neither was misleading nor material. First, the defendant claims that SA Fallon "made it appear as though the user of the Defendant's IP address had registered for an account with the Target Site" by including facts related to what a user could do, user data and images trafficked by users, Def. Mot. at 12, and misled the Magistrate Judge by failing to indicate that he was not in possession of evidence showing that the Target IP Address user was a registered user of the Target Website. However, when put in the context of the full affidavit, the defendant's claims fail. SA Fallon included the user information cited by the defendant in the section of the affidavit where he accurately described the Target Website. *See* Def. Ex. E, ¶¶ 15-18. This was a description of the Target Website in general, not as it was used or accessed by the Target IP Address user. That section was separate from the next section titled, in bold, "Evidence Related to

Identification of Target that Accessed Target Website." *Id.* at p. 13. In the latter section, which focused on the actions of the Target IP Address user, SA Fallon included information as to what users with and without an account could access. *See id.* at ¶ 20. Nowhere in the affidavit did SA Fallon claim that the Target IP Address user is a registered user of the Target Website, nor did he ask the Court to reach that conclusion. SA Fallon could not make that representation because the FLA did not provide registration or account information to the FBI. However, failing to state that such evidence was not provided to the FBI was not a knowing or reckless omission that would mislead the Magistrate Judge. Rather, a common-sense conclusion drawn from the affidavit would be that the FBI was not in possession of such evidence and information, because if it was, it would have included it in the affidavit. SA Fallon provided an accurate recitation of the facts and the Magistrate Judge was at liberty to draw his own conclusion based on those facts.

Second, the defendant claims that SA Fallon misled the Magistrate Judge by failing to include that the Target IP Address was not registered with NCMEC, the defendant had no criminal history and was not a sex offender and that database searches did not identify derogatory information about the defendant. Again, the defendant provides no evidence that SA Fallon omitted this information to knowingly or recklessly mislead the Magistrate Judge. Furthermore, the Magistrate Judge likely was not mislead because, again here, common sense would lead the Magistrate Judge to conclude that because a relevant criminal history was not provided, one does not exist. Nor was the omission material to the Magistrate Judge's probable cause determination. The defendant's lack of a criminal history does not negate the fact that the FLA identified the Target IP Address user, at the subject premises, as accessing the Target Website. "Accessing child sexual abuse and exploitation material violates the law regardless of whether" an individual has broken similar or any laws in the past. *See Sanders*, 1:20-cr-00143 (TSE), Dkt. No. 122 at 17.

The remainder of the points raised by the defendant have been addressed above, including that SA Fallon did not knowingly or recklessly mislead the Magistrate Judge by: (1) concluding that "there is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE," where the facts in the affidavit showed that the FLA identified, through its investigation, the IP address that actually accessed the Target Website, and that IP address was registered to the defendant at the subject premises; or (2) including language as to the characteristics of those who possess and access with the intent to possess child pornography, because the facts set forth elsewhere in the affidavit supported the conclusion that the Target IP Address user purposely accessed the Target Website through Tor, thereby exhibiting characteristics consistent with a collector of child pornography—thus this was not inappropriate or heedless boilerplate language. Furthermore, the defendant again provides no proof to support his allegations the contrary.

C. THE DEFENDANT'S CONFESSION IS ADMISSIBLE

While said in other words, the defendant argues that his written and recorded confessions must be suppressed as the fruit of the poisonous tree. *See* Def. Mem., Dkt. No. 44 at 14. Specifically, the defendant argues that his non-custodial and post-*Miranda* statements were the result of the search that he claims was not supported by probable cause. However, the tree here was not poisonous. As set forth in Section A above, the search warrant was supported by probable cause, and even if it was not, as set forth in Section B, officers executed the search warrant in good faith. Therefore, evidence and statements resulting from the search should not be suppressed, including the defendant's non-custodial and post-*Miranda* written and recorded admissions.[9]

[9] It does not appear that the defendant is otherwise contesting the admissibility of his non-custodial and post-*Miranda* admissions. Should the defendant make such an argument, the government requests

CONCLUSION

For the reasons set forth above, the defendant's motion to suppress evidence and statements should be denied without a *Franks* hearing.

the ability to respond, as it is the government's position that the statements are admissible on all grounds.